

REMARKS

This application has been reviewed in light of the Office Action mailed on April 2, 2004. Claims 1-10 are pending in the application with Claim 1 being in independent form. By the present Amendment, Claims 1-2 and 4-10 have been amended, Claim 3 has been cancelled. No new matter or issues are believed to be introduced by the amendments.

Claims 1-10 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,917,908 issued to Takenaka Anderson on June 29, 1999.

In the Office Action, the Examiner states that, as per claims 1 and 8-10, Takenaka teaches a method of copy-protection services on a storage medium characterized in that data on the storage medium are encrypted with a key which depends on a position of data in the memory module and that in each write operation (storing a file) data is written into positions on the storage medium that are chosen at random.

In response, the limitations of Claim 3 have been incorporated into independent Claim 1. In addition, Claim 1 has been further amended to clarify the claimed subject matter over Takanaka. It is respectfully submitted that Claim 1, as amended, is patentable over Takenaka for at least the following reasons.

Takenaka teaches a file protection system for protecting a file stored in a storage unit. In an installing process, machine specific information, which is information specific to a user system is generated. The method for generating the machine specific information is taught in Takanaka at Col. 5, lines 35-45:

Referring to FIG. 6, random numbers are generated and a predetermined number of random numbers are selected from among the generated random numbers. A number in which respective digits are formed of the selected random numbers is used as the machine specific information. In addition, by using the generated random numbers, an address at

which a file is stored in the storage unit 20 is decided (S112). Since addresses at which files are stored in the storage unit 20 are decided by using the random numbers, the files can be stored in the storage unit 20 at random. [Emphasis Added]

As described at Col. 5, lines 35-45 of Takanaka, a random number is selected, referred to in Takanaka as “machine specific information”, (positional-information item k), used to determine an address at which a file is stored in the storage unit. After determining the address at which a file is stored in the storage unit, Takanaka teaches that another file is opened for the purpose of writing the “machine specific information“. To provide copy protection, Takanaka teaches that positional-information item k is added to the data to be stored. Positional-information item k and the data to be stored are integrated and encrypted using a secret key given to the user. The encrypted data is written in an area identified by the positional-information item k. After this, other information is written to the respective areas identified by positional-information items i and j in a file-name management portion and a data management portion of the storage medium. At a later time, when the file of the machine specific information is opened, positional-information items i', j' and k' are retrieved based on the file name. At this point, positional-information item k' (the position of the actual storage location of the file) is compared with positional-information item k (the position of the originally intended storage location), obtained by the decryption process. In the case where the positional-information items k and k' are equal, the file is closed. On the other hand, in the case where they differ, an error signal is output indicating that the file has been unjustly moved or copied from another system.

It is respectfully submitted that in Takanaka does not disclose the subject matter of Claim 1. Specifically, there is no disclosure or suggestion in Takanaka of performing separate write operations for each data block of a file to positions on a storage medium chosen at random, as recited in Claim 1.

Claim 1 as amended herein recites:

A method for providing copy-protection to data stored on a storage medium, wherein the data stored on the storage medium is arranged in blocks, in each block write operation, a data block is written into a position on the storage medium that is chosen at random; and wherein each of said data blocks to be written on said storage medium are encrypted with a key K which is derived from a position of one or more data blocks on the storage medium and a shared secret S. [Emphasis Added]

In Takanaka, as described above, a single random number, k, is used as machine specific information to determine whether the file has been unjustly moved or copied from another system.

By contrast, the presently claimed invention operates at a different level than that described by Takanaka. Specifically, a unique random number is determined for each data block of a stored file to store the individual data blocks in the storage medium.

Further, the plurality of unique random numbers associated with the respective data blocks are used to encrypt the data blocks with a key which is dependent in part on the randomly determined locations. In this manner, a relation is created between the location of the data and a decryption key. Copying will change the storage location, and in consequence will break the relation between location and decryption key.

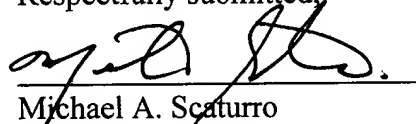
Accordingly, applicant respectfully request withdrawal of the rejection under 35 U.S.C. §103(a) with respect to Claim 1 and allowance thereof is respectfully requested.

Claims 2 and 4-10 depend from independent Claim 1 and therefore contain the limitations of Claim 1. Hence, for at least the same reasons given for Claim 1, Claims 2 and 4-10 are believed to be allowable over Takanaka. Accordingly, withdrawal of the rejection under 35 U.S.C. §103(a) with respect to Claims 2 and 4-10 is respectfully requested.

In view of the foregoing amendments and remarks, it is respectfully submitted that all claims presently pending in the application, namely, Claims 1-2 and 4-10 are believed to be in condition for allowance and patentably distinguishable over the art of record.

If the Examiner should have any questions concerning this communication or feels that an interview would be helpful, the Examiner is requested to call Dicron Halajian, Esq., Intellectual Property Counsel, Philips Electronics North America, at 914-333-9607

Respectfully submitted,



Michael A. Scaturro

Reg. No. 51,356

Attorney for Applicant

Mailing Address:
Intellectual Property Counsel
Philips Electronics North America Corp.
P.O. Box 3001
345 Scarborough Road
Briarcliff Manor, New York 10510-8001